MEDIA DEVELOPMENT & DIVERSITY AGENCY

Annexure B

RISK MANAGEMENT STRATEGY

FOR

2022/23 –2024/25 FINANCIAL YEARS

A. STRATEGY APPROVAL

Document title	Risk Management Strategy					
Document author	Chief Executive Officer					
Synopsis	This document contains the MDDA Risk Management Strategy					
Document owner	Chief Risk Officer					
Document description	To set a strategic approach and guide the implementation of risk management activities in the Agency.					
Final Version	VI					
Number of pages	20					
Recommended by the Chief Executive Officer	Full acceptance		Partial acceptance		Conditional acceptancel	
Signature: **Date:**	30 April 2023					
Recommended status by the Audit and Risk Committee	Full approval		Partial approval		Conditional approval	
Signature: **Date:**						
Acceptance status by the Board	Full approval		Partial approval		Conditional approval	
Signature: **Date:**	21/07/2023					

B. LOCATION OF THE MASTER FINAL VERSION OF THE STRATEGY

(AFTER SIGNATURE BY THE ACCOUNTING AUTHORITY) To facilitate future access and use the master final version of Risk Management strategy, the original signed strategy will be archived on file in Registry; an Adobe Acrobat (pdf) copy will be placed on the intranet. This strategy and any amendments thereto become effective upon the approval of the Board. **(Annexure A).**

TABLE OF CONTENTS

1. Preamble

1.1 The Media Development and Diversity Agency (MDDA); established in 2003 in terms of the MDDA Act No. 14 of 2002; is a statutory development agency for promoting and ensuring media development and diversity.

1.2 The Accounting Authority of Media and Diversity Agency (MDDA) is committed to a process of risk management that is aligned to the principles of good corporate governance, as supported by the Public Finance Management Act, 1999 (PFMA), (Act No. 1 of 1999) as amended by Act 29 of 1999.

1.3 Risk management is a valuable management tool which increases the Agency's prospects of success through minimising the negative impact and optimising opportunities emanating from its operating environment.

1.4 Risk management is ideally positioned to ensure that challenges facing the Agency are managed effectively. It adds value to the Agency by systematically identifying, assessing, prioritising, monitoring, and evaluating key risks in a systematic disciplined approach.

1.5 Risk management is a strategic imperative in the organisation and ensures that it sets clear and realistic objectives, understands critical risks associated therewith and develops mitigation strategies to manage such risks.

1.6 The Agency recognises the King IV Report on Corporate Governance as best practice. It requires that the Agency should establish a risk management structure that will adequately identify, measure, monitor and control the risks involved in its various operations and lines of business.

1.7 The Agency commits to all risk management principles as defined in the Public Sector Risk Management Framework to ensure that resources are managed efficiently and effectively promote the following:

- Risk management is an enterprise-wide approach which means that risk management will form an integral part of the entity's business processes.
- The MDDA sets clear goals and understands the critical risks associated with them.
- Strategic risks are managed to ensure client and stakeholder expectations are met.
- Ensure more sustainable and reliable delivery of services.

1.8 This strategy must be read in conjunction with the MDDA's *Risk Management Policy*.

2. Legislative Mandate

2.1 Managing risks is fundamental to the business of the entity. The PFMA through section 38(1)(a)(i) requires the Accounting Officer/ Authority to ensure that the MDDA has and maintains effective, efficient, and transparent systems of financial and risk management and internal control.

2.2 Section 45 of the PFMA further extends the general responsibilities for internal control, risk management and financial management to employees at all levels in the organisation.

2.3 Section 3.2.1 of the Treasury Regulations states that the Accounting Officer/Authority must ensure that a risk assessment is conducted regularly to identify emerging risks of the institution.

2.4 A risk management strategy, which must include a fraud prevention plan, must be used to direct internal audit effort and priority, and to determine the skills required of managers and staff to improve controls and to manage these risks. The strategy must be clearly communicated to all officials to ensure that the risk management strategy is incorporated into the language and culture of the institution.

3. Objectives

3.1 The objectives of the Risk Management Strategy are to:

- To define the principles and approach of the Agency's Risk Management processes which will be used to effectively identify, assess, measure, treat and monitor risks in order to meet business and strategic objectives.
- To provide guidance to management and staff as to how risks should be managed.
- Provide a sound basis for integrated risk management and internal control as components of good corporate governance.
- Ensure that risk management is clearly and consistently integrated and evidenced in the culture of the MDDA.
- To provide a level of assurance that current significant risks are effectively managed.

4. Enterprise-wide approach to managing risks

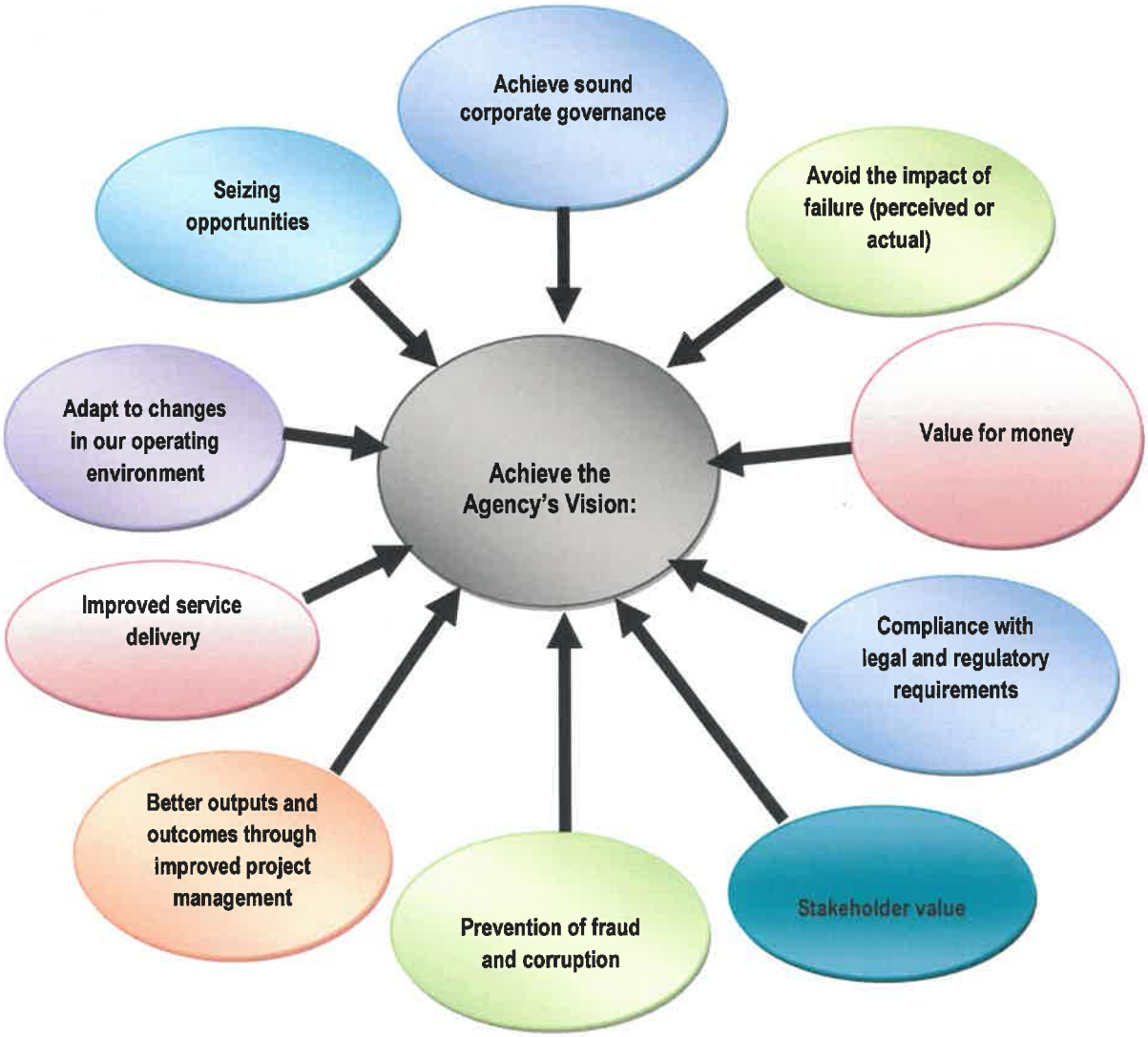
4.1 Enterprise Risk Management (ERM) recognises that risks (including opportunities) are dynamic, often highly interdependent and ought not to be considered and managed in isolation. It is the application of risk management throughout the organisation, rather than only in selected business areas or disciplines. All organisations face uncertainty to varying degrees. ERM responds to this challenge by providing a methodology for managing organisation-wide risks in a comprehensive and integrated way.

4.2 Our stakeholders expect value from interfacing with us. The ERM acknowledges that this value is created, preserved, or eroded by management decisions at strategic and operational levels. Understanding the uncertainties in the entity's operating environment enables management to take better informed decisions thereby enhancing the stakeholder value.

4.3 In order to plan effectively, the entity needs to set clear goals, understand the risks associated with achieving the set goals and analyse the impact of these eventualities and probabilities on the performance of the organisation.

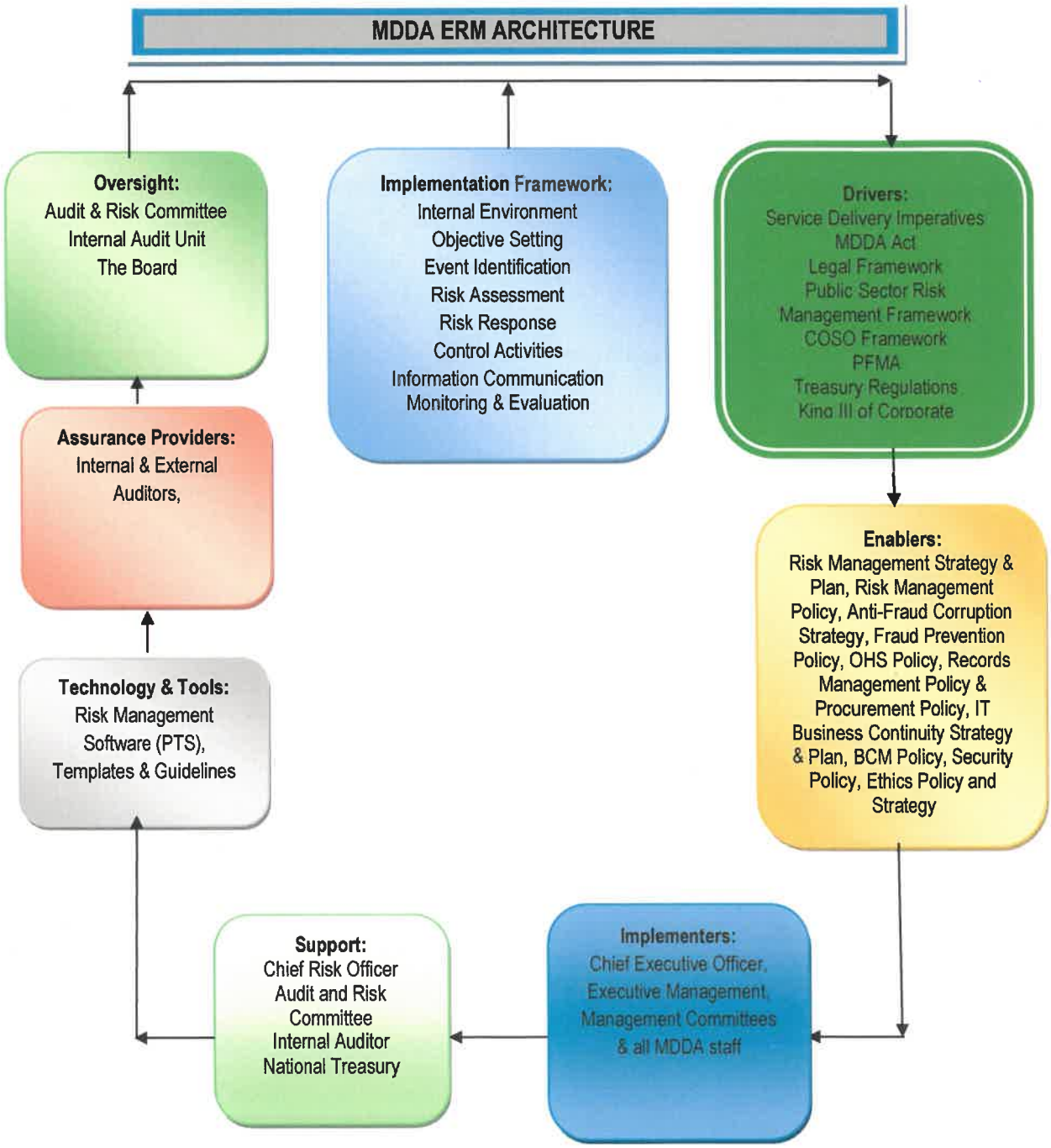
Figure 1 below provides an illustration of the benefits of ERM for the MDDA.

Figure 1: The benefits of ERM for the Agency



In line with the Public Service Risk Management Framework, the MDDA has adopted the following ERM architecture as a model for management of risks:

Figure 2: The MDDA's ERM Architecture Model



5. The Agency's Risk management process

The MDDA's risk management process is in accordance with Public Sector Risk Management Framework which is aligned with the COSO framework articulated as follows:

5.1 Control Environment

5.1.1 Internal controls are a key element to management of risks by management. They include both financial and non-financial control (e.g., annual leave records and controls in place to safeguard misuse of MDDA assets including computer systems, etc).

5.1.2 Management is responsible for ensuring that there are appropriate and adequate internal controls in the organisation to ensure an efficient and effective risk management implementation. The financial and non-financial policies and regulations (legislations) are one example of these controls.

5.1.3 The MDDA's financial and other non-financial procedures are the definitive guide and are available to all staff. It is the responsibility of management to ensure that controls in their areas of responsibility have been documented and communicated to all.

5.1.4 In order to set a good example, managers should comply with internal controls. The emphasis should be on creating a culture of honesty and fraud detection, not increasing the volume of detailed operational and supervisory checks and controls, unnecessarily.

5.1.5 Ethical values are intertwined with risk management and management processes.

5.2 Objective Setting

5.2.1 Risk identification shall be based on the MDDA's objectives as outlined in the strategic plan and chosen objectives that support and align with the organisation's mission. The objectives

must be consistent with risk appetite and tolerance levels. Risks threatening the strategic achievement of objectives shall be identified annually for each programme.

5.3 Risk Identification

5.3.1 Methodology to be used in the identification of risks will be agreed upon prior to the commencement of the process. The Chief Risk Officer shall facilitate the identification of risks process. Emerging risks for programmes or business units will be identified regularly and reported to the Chief Risk Officer, for presentation to the Audit and Risk Committee and the Board.

5.4 Risk Assessment

5.4.1 Risk assessment is a formal and systematic approach to conduct a detailed examination and evaluation of the organisational risks and exposure. The MDDA's risk registers will be updated continuously at least twice a year and reviewed formally annually. A zero (0) based risk assessment will be performed after every three years or when the need arises.

The risk assessment process shall include the following 4 steps:

Step 1: Quantifying the parameters (scoring system) of impact and likelihood before the actual assessment (see tables below):

Risk Rating Tables

5.5 The organisation's risk appetite

5.5.1 MDDA's risk appetite and tolerance levels will be detailed in the Tolerance and Appetite Statements.

5.5.2 The tables below highlight the levels of risk and their tolerance levels.

Step 4: Determine the risk acceptability and action will be proposed to reduce the risk (see table below)

a) Likelihood

Likelihood is the probability (considering the present control environment or action in hand) that an adverse event, which could cause materialisation of the risk, rated as follows:

Rating	Likelihood Category	Definition
5	Almost certain	The risk is almost certain to occur in the current circumstances. The risk is already occurring or is likely to occur more than once within the next 12 months.
4	Likely	The risk or opportunity could easily occur and is likely to occur at least once within the next 12 months. More than an even chance of occurring.
3	Possible	Could occur quiet often. There is an above average chance that the risk or opportunity will occur at least once in the next 3 years.
2	Unlikely	Small likelihood but could happen. The risk occurs infrequently and is unlikely to occur within the next 3 years.
1	Rare	Not expected to happen – event would be a surprise. The risk is conceivable but is only likely to occur in extreme circumstances.

Step 2: Applying the parameters to the risk matrix to indicate what areas of risk matrix would be regarded as catastrophic, critical, Serious, Significant or minor (see table below):

b) Impact

Impact is the potential loss to the organisation should the risk materialize, rated as follows:

Impact Category	Continuity of Service Delivery	Safety & Environmental
Catastrophic	Risk event will result in widespread and lengthy reduction in continuity of service delivery to stakeholders of greater than 48 hours.	Major environmental damage. Serious injury (permanent disability) or death of personnel or members of the public. Major negative media coverage.
Critical	Reduction in service delivery or disruption for a period ranging between 24 & 48 hours over a significant area,	Significant injury of personnel or public. Significant environmental damage. Significant negative media coverage.
Serious	Reduction in service delivery or disruption for a period between 8 & 47 hours over a regional area.	Lower-level environment, safety or health impacts. Negative media coverage.
Significant	Brief local inconvenience (work around possible). Loss of an asset with minor impact on operations.	Little environmental, safety or health impacts. Limited negative media coverage.
Minor	No impact on business or core systems.	No environmental, safety or health impacts and/or negative media coverage.

Inherent Risk

Inherent risk is defined as the exposure arising from risk factors in the absence of deliberate management intervention(s) to exercise control over such risk factors.

Inherent risk rating = impact x likelihood (in the absence of mitigating controls)

Residual Risk

Residual risk is defined as the remaining exposure after the mitigating effects of deliberate management interventions(s) to control such exposure (the remaining risk after management has put in place measures to control the inherent risk.)

The table below was used to assist management in quantifying the adequacy of existing risk mitigating controls, in order to determine the residual risk:

Risk rating	Effectiveness category	Category Description	Factor
5	Very good	Risk exposure is effectively controlled and managed.	90%
4	Adequate	Majority of risk exposures is effectively controlled and managed.	80%
3	Partially adequate	There is a room for some improvement in the control system.	50%
2	Inadequate	Some of the risk exposures appear to be controlled, but there are major deficiencies.	20%
1	Unsatisfactory	Control measures are ineffective.	10%

Residual risk = inherent risk – control adequacy rating.

In order to assist in determining the extent of inherent and/or residual risk, the following scales will be used:

Inherent and/or Residual risk rating scales

Inherent risk category	Category Description	Factor
Extreme	The risk must be shared (insured), terminated or controlled.	21 up to 25
High	This risk should be shared (insured) or controlled.	>15 up to20
Moderate	This will typically be controlled (treated)	>11 up to 15
Within risk tolerance	Management will make an informed decision as to where this risk must be controlled or absorbed by the Board. The decision will be based on a 'cost vs benefit' approach.	>6 up to 10
Within risk appetite	Impact and probability are insignificant. This risk may be tolerated, and cost of losses will be absorbed by the Board.	Up to 5

5.7 Risk Indicator Assessment

5.7.1 The organisation has set a risk indicator to measure early warning and to identify potential events that may harm continuity of the activity/project and provides information on the level of exposure to a given operational risk for the Agency. The risk indicator has to have an explicit relationship to the specific risk whose exposure it represents.

Risk Management Reporting Assessment per KRI will be as follows:

%	Risk Level
0-8%	
8-12%	
> 12	

Roles and Responsibilities setting and Managing RPI's are outlined as follows:

Management	Risk Management	Internal Audit
Identification of indicators.	Provide guidance and challenge the selection of KRIs and thresholds.	Provide validation/ independent assurance around the KRI process.
Setting of thresholds.	Quarterly reporting on KRI breaches.	Incorporate outputs into audit plan.
Monitor position against targets and limits.	Escalation reporting to the Audit and Risk Committee and the Accounting Authority.	N/A

Escalate breaches to operational risk management.	Identify and analyse trends across the organisation.	N/A

5.7.2 Risk Response Matrix

Impact	I – Contingency Plan/Transfer	IV – Critical Treat/Transfer/Terminate
	IV – Minor Monitor/Tolerate	III – Housekeeping Treat/Tolerate

Likelihood

5.8 Risk Treatment Options:

The organisation's appropriate risk management response plan for each risk shall be identified and be classified under the following categories:

5.8.1 Terminate Risk

This involves the organisation's decision not to proceed with particular programme or project or even choosing an alternative way of achieving the same outcome.

5.8.2 Risk Tolerance

This involves the organisation taking no action to affect the likelihood or impact because it is such a minimal risk or the cost to implement the risk is too high relative to the cost of the risk.

5.8.3 Risk Transfer

This involves the organisation sharing responses/reducing risks likelihood or impact by transferring or otherwise sharing the portion of the risk. Insuring the risk is another form of risk transfer and might involve taking out an insurance policy.

5.8.4 Risk Control

This involves the organisation reducing the likelihood by putting in place appropriate internal control arrangements.

Adequacy of the risks' response plan for the organisation's top risks shall be reviewed by management to ensure that strategies will reduce risks to an acceptable level. The Management and Audit and Risk Committees shall review the adequacy for medium and high-risk response plan to ensure that the strategies will reduce risk to an acceptable level. Risk register shall include risk response plans.

5.9 Control Activities

5.9.1 Each risk response plan will be addressed through the development of related internal controls and/or implementation procedures. Each unit shall provide a report on the implementation of risk response plan to the Management Committee (Manco) and to the Audit and Risk Committee. The Management Committee shall report to the Audit and Risk Committee and the Board on the implementation of risk response plan for the identified risks.

5.9.2 Managers shall coordinate the reporting of the implementation process to the Chief Risk Officer. The Management Committee shall report the implementation of risk response plan to the Chief Executive Officer.

5.10 Information and Communication

5.10.1 Managers shall assist with the coordination of risk management matters and communication of the risks to staff. The Audit and Risk Committee shall ensure the existence of an information system for recording risks response plan/control activities for the organisation.

5.10.2 The Chief Risk Officer shall conduct research on the appropriate information system for recording the organisation risks response plan/control activities and advise the Audit and

Risk Committee accordingly. All identified risks threatening the achievement of objectives shall be communicated to the Accounting Authority.

5.11 Monitoring

5.11.1 Internal Audit shall formally review the effectiveness of risk management process. The internal audit plan (three year and annual coverage) shall be risk-based and high risks shall be prioritised. The internal audit unit shall evaluate the effectiveness of risk response plan.

5.11.2 The Office of Auditor-General shall conduct independent review of internal controls, risk management and governance processes. The Audit and Risk Committee shall report to the Board activities undertaken by the organisation on the risk management issues.

5.12 Communication and Reporting

5.12.1 The Chief Risk Officer will prepare reports to the Management and Audit and Risk Committees in line with the organisation's Risk Management Reporting Framework on a quarterly basis and the Chairperson of the Audit and Risk Committee will report to the Accounting Authority on a regular basis. The Audit and Risk Committee Chairperson's report will seek to keep the Accounting Authority up to date on performance, emerging risks and the functioning of risk management and other relevant events and issues.

6. RISK MANAGEMENT RESOURCES PLAN

6.1 Personnel

6.1.1 The Public Sector Risk Management Framework recommends that risk management unit is represented by the requisite number of people with the right skills. Adequate capacitation of this unit is fundamental to implementing the risk management strategy.

6.1.2 The organisation has an appointed Internal Auditor, Chief Risk Officer and Audit and Risk Committee and reports risk intelligence to the Accounting Authority. Figure 4 below illustrates the current structure for the risk management unit.

Figure 4: Risk Management Structure:

6.2 Risk Management Office

6.2.1 The Chief Risk Officer is the primary custodian of risk management processes in the organisation. The Chief Risk Officer is to be responsible for coordination and analysis of information needed to advise the Management and Risk and Audit Committees as well as the Board on risk management processes in the entity.

6.3 Relationship with Internal Audit

6.3.1 The relationship between the Risk Management unit and Internal Audit unit must be detailed in the Internal Audit methodology / Charter. The Internal Audit unit and the Risk Management unit will partner office in:

- The organisation's risk exposure when they conduct internal audit review and when they give input on the quarterly risk management performance reports.

- Monitoring and evaluating the effectiveness and efficiency of risk management activities.

7. Risk Ownership

7.1 The overall ownership of risk management in the organisation lies with the Accounting Authority. The Executive Management (CEO, Directors, and CFO) are risk owners in the respective divisions or units and responsible for ensuring that risk management is implemented effectively, efficiently and economically.

8. Strategy Implementation & Review

8.1 The strategy shall upon approval by the Accounting Authority be communicated to all staff members through internal communications platforms and will also be made available on the intranet. The Risk Management Implementation Plan for 2022/23 will be attached to this strategy and reviewed as and when a need arises. (Annexure A).

9. Glossary of Terms

Basic Term	Definition
MDDA	Media Development and Diversity Agency
PFMA	Public Finance Management Act (Act No. 1 of 1999 as amended by Act No. 29 of 1999).
Framework	The Public Sector Risk Management Framework.
Executive Authority	The Cabinet member who is accountable to Parliament for that The Agency.
Accounting Authority	Chief Executive Officer
Accounting Authority	The Board of the MDDA
Risk	An unwanted outcome, actual or potential, to the institution's service delivery and other performance objectives, caused by the presence of risk factor(s).
Inherent Risk	The exposure arising from risk factors in the absence of deliberate management interventions to exercise control over such factors.
Residual Risk	The remaining exposure after the mitigation effects of deliberate management intervention(s) to control such exposure (the remaining risk after management has put in place measures to control the inherent risk).

Risk Factor	Any threat or event which creates or has the potential to create risk.
Risk Bearing Capacity:	The maximum amount of risk that the institution is able to accept in line with government priorities, its strategic goals, without exposing it to the point where its survival is under threat and faces financial constraints.
Risk appetite	The amount and type of risk that the institution is willing to accept in line with its strategic goals.
Risk Tolerance	The amount of risk the institution is capable of bearing (as opposed to the amount it is willing to bear).
Enterprise risk Management:	A process applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of the organisation's objectives.